

Abstract of the Disclosure

~~In a method for modular multiplying a~~ A multiplicand is multiplied by a multiplier using a modulus. [[, the]] ~~The~~ multiplicand, the multiplier and the modulus being are polynomials of variable. [[, a]] ~~A~~ multiplication look-ahead method to obtain a multiplication shift value is carried out. An intermediate result polynomial is shifted to the left by the number of digits of the multiplication shift value ~~to~~ obtain a shifted intermediate result polynomial. Furthermore, a reduction look-ahead method to obtain a ~~A~~ reduction shift value is carried out, the reduction shift value equalling the difference of the degree of the shifted intermediate result polynomial and the degree of the modulus polynomial is obtained in a reduction look-ahead method. The modulus polynomial is then shifted by a number of digits equalling the reduction shift value ~~to obtain a shifted modulus polynomial~~. In a three-operands addition, the shifted ~~intermediate result~~ polynomial and the multiplicand are summed and the shifted modulus polynomial is subtracted ~~to obtain an updated~~ ~~intermediate result polynomial~~. ~~By iteratively executing the~~ ~~preceding steps the~~ The modular multiplication is are iteratively executed and processed progressively until all the powers of the multiplier polynomial have been processed. ~~By~~ ~~means of~~ With a carry disabling function ~~it is possible to~~ ~~carry out both a~~ Z/NZ arithmetic as well as a and GF

Appl. No. 10/623,830
Amdt. dated September 24, 2004
Reply to Office action of June 24, 2004

arithmetic can be carried out on a single long number
calculating unit.

Fig. 2